G.E.T SECURE ID CORP.
230 Third Ave., Waltham, MA 02451 USA

15th November 2024

Subject: Confirmation of conformity of iOS-based mDL - GET Mobile ID, v.5.4.8 with ISO/IEC 18013-5:2021

Dear Mr. Joshua,

This letter serves to confirm the conformity of the abovementioned mDL application ('the application') to ISO/IEC 18013-5:2021.

FIME tested v.5.5.1(13) of this mDL application in January 2023 and found it to be compliant with this standard. The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page. The number of the Test Report containing the full overview of executed test cases and all test results is UL_eID_GET_iOS_003.

In August 2024, G.E.T SECURE ID CORP provided Fime with release notes describing the changes between the tested version 5.4.8 and version 5.5.1(13). After reviewing these release notes, FIME concluded there is no need for re-testing version 5.4.8 since the described changes are not likely to impact the conformity to ISO/IEC 18013-5.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. G.E.T SECURE ID CORP is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

This confirmation letter is valid for one year from the date of issuance.

Yours sincerely,

FIME

David Bakker
Technical Lead

mDL implementation scope

System Under Test

Application name and version	mDL - GET Mobile ID, v.5.5.1 (13)
Operating System	iOS
Application available through	TestFlight
Date of receipt of application	2023-01-09
Certification Type	Integrated Product Certification
Issuing Authority	Utah Driver License Division

Implementation Conformance Statement Summary

Device engagement technologies	QR code
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode
Server retrieval technologies	WebAPI, OIDC
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test Suite	UL mDL Application Test Suite v1.1.12
mDL Test App	mdltestapp-1.1.4
Test device on which the mDL Test App is installed	Google Pixel 3a
OS version of the test device on which the mDL Test App is installed	Android 12

Test Devices and Platform

Device brand and type	iPhone 13	iPhone SE (2nd Gen)
OS version	iOS 16.2	iOS 13.5.1

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by G.E.T SECURE ID CORP and have been used to determine which test cases to execute.

The ICS version used by GET Group is v1.5.

A.1.1 General information

mDL owner	
Application owner Name	G.E.T SECURE ID CORP.
Address	230 3rd Avenue
City	Waltham
State	MA
Zip Code / Postal Code	02451
Country	USA
Contact Name	Joshua M Marmol
Contact Title	Managing Director
Contact Email Address	JMarmol@getgroup.com
Contact Phone Number	+1 617-775-5407

Issuing Authority General Information (Applicable for Integrated Product Certification Only)	
Issuing Authority Name	Utah Department of Public Safety, Driver License Division
Issuing Authority Address	Utah Department of Public Safety
City	Salt Lake City
State	Utah
Zip Code / Postal Code	84114-4501
Country	USA
Contact Name	Brittaney Akagi
Contact Title	IT / Quality Assurance Manager
Contact Email Address	bakagi@utah.gov

mDL Application General Information	
Certification Type	☐ Functional[1] ☒ Integrated Product[2]
Application name and version	GET Mobile ID, v.5.5.1 (13)
The minimum version of iOS supported	13.4
How many documents are present on the mDL under test?	1

[1] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.

[2] Integrated product certification requires the mDL data set to be prepared and personalized by an Issuer System of Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.

For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva

For each namespace different from the mDL namespace (“org.iso.18013.5.1”), please specify the identifiers of all data elements present in the document	{
	"org.iso.18013.5.1.mDL" : {
	"com.scytales.18013.5.1" : [
	"status",
	"vehicle_category",
	"vehicle_category_list",
	"full_address",
	"email",
	"mobile_number"
	],
	"org.aamva.us" : [
	"real_id"
	],
	"org.iso.18013.5.1.aamva" : [
	"DHS_compliance"
	]
	}
	}

A.1.2 For mdl data model test cases

Note: all the data elements in this section are in the default mDL data namespace (“org.iso.18013.5.1”). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases [3]	
1.	Data element administrative_number is present in the mDL data.	☒YES ☐NO
2.	Data element sex is present in the mDL data.	☒YES ☐NO
3.	Data element height is present in the mDL data.	☒YES ☐NO
4.	Data element weight is present in the mDL data.	☒YES ☐NO

[3] Note: all of the data elements in this section are in the default mDL data namespace (“org.iso.18013.5.1”). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

5.	Data element eye_color is present in the mDL data.	☒YES ☐NO
6.	Data element hair_color is present in the mDL data.	☒YES ☐NO
7.	Data element birth_place is present in the mDL data.	☒YES ☐NO
8.	Data element resident_address is present in the mDL data.	☒YES ☐NO
9.	Data element portrait_capture_date is present in the mDL data.	☒YES ☐NO
10.	Data element age_in_years is present in the mDL data.	☒YES ☐NO
11.	Data element age_birth_year is present in the mDL data.	☒YES ☐NO
12.	Data element age_over_NN is present in the mDL data. In case you select YES, please provision the following age_over_NN data elements in the mDL data with the corresponding values (TRUE / FALSE) during personalization.	☒YES ☐NO
	NN	**Return Value**
	age_over_15	TRUE
	age_over_18	TRUE
	age_over_21	TRUE
	age_over_60	FALSE
	age_over_65	FALSE
	age_over_68	FALSE
13.	Data element issuing_jurisdiction is present in the mDL data.	☒YES ☐NO
14.	Data element nationality is present in the mDL data.	☒YES ☐NO
15.	Data element resident_city is present in the mDL data.	☒YES ☐NO
16.	Data element resident_state is present in the mDL data.	☒YES ☐NO
17.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO
18.	Data element resident_country is present in the mDL data.	☒YES ☐NO
19.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO

20.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
21.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
22.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
23.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
29.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
30.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
38.	Data element family_name_national_character is present in the mDL data.	☒YES ☐NO

39.	Data element given_name_national_character is present in the mDL data.	☒YES ☐NO
40.	Data element signature_usual_mark is present in the mDL data.	☒YES ☐NO

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
41.	mDL supports device engagement using NFC Static Handover	☐YES ☒NO
42.	mDL supports device engagement using NFC Negotiated Handover [4]	☐YES ☒NO
43.	mDL supports device engagement using QR code	☒YES ☐NO
44.	mDL supports device retrieval using NFC	☐YES ☒NO
45.	mDL supports extended-length APDUs for device retrieval using NFC	☐YES ☒NO
46.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension	☒YES ☐NO
47.	mDL supports device retrieval using BLE in mdoc central client mode	☒YES ☐NO
48.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic	☒YES ☐NO
49.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE	☐YES ☒NO
50.	mDL supports device retrieval using BLE in mdoc peripheral server mode	☒YES ☐NO
51.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE	☐YES ☒NO
52.	mDL supports device retrieval using Wi-Fi Aware	☐YES ☒NO
53.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware [5]	☐YES ☒NO

[4] Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies

[5] Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

54.	mDL supports server retrieval using OIDC	☒YES ☐NO
55.	mDL supports server retrieval using WebAPI	☒YES ☐NO
56.	mDL supports transferring server retrieval information in the device engagement structure	☒YES ☐NO
57.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message	☐YES ☒NO
58.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	

A.1.4 For security mechanism test cases

	ICS statements for Security Mechanisms test cases	
59.	Which curves does the mDL support for session establishment? Tick all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
61.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
62.	Which curves does the mDL issuing authority support for issuer data authentication? Tick all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

[6] If the mDL supports multiple curves for session establishment, then for the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

[7] If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that UL expects the same curve to be used

63.	The mDL supports mdoc MAC authentication.	☒YES ☐NO
64.	If yes, which curves does the mDL support for mdoc MAC authentication? Tick all that are supported [8]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
65.	The mDL supports mdoc ECDSA/EdDSA authentication	☒YES ☐NO
66.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Tick all that are supported[9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
67.	The mDL supports mdoc reader authentication	☒YES ☐NO

for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[8] If multiple documents are present on the mDL, the mDL can, in theory, use a different mdoc MAC authentication curve for each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[9] Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that UL expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, UL expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

68.	If yes, which curves does the mdoc support for mdoc reader authentication? Tick all that are supported[10].	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

69.	If yes, for which data elements is successful reader authentication required before the mdoc will release them[11]	{
		"org.iso.18013.5.1.mDL" : {
		"org.iso.18013.5.1" : [
		"administrative_number",
		"sex",
		"weight",
		"eye_colour",
		"hair_colour",
		"birth_place",
		"resident_address",
		"portrait_capture_date",
		"age_in_years",
		"age_birth_year",
		"age_over_15",
		"age_over_18",
		"age_over_21",
		"age_over_60",
		"age_over_65",
		"age_over_68",
		"issuing_jurisdiction",
		"nationality",
		"resident_city",
		"resident_state",
		"resident_postal_code",
		"resident_country",
		"family_name_national_character",
		"given_name_national_character",
		"signature_usual_mark
		] } }

70.	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	☐YES ☒NO

[10] UL assumes that all mDL samples provided to us will support all of the mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

[11] UL assumes that if mdoc reader authentication is supported, there is at least one data element that will not be released if mdoc reader authentication is not performed or fails.

A.1.5 For use case test cases

#	ICS statements for Use Case test cases	
71.	The mDL allows the mDL holder to refuse consent for sharing the portrait data element if requested by the reader	☐YES ☒NO